

In re Patent Application of:

MACCHETTI ET AL.

Serial No. 10/816,791

Confirmation No. 9927

Filed: **APRIL 2, 2004**

REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 12, for example, is directed to a method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function. The method comprises decoding an input byte and generating at least one bit string that contains only one active bit, and logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string, and encoding the 256-bit string for obtaining an output byte.

The method may be advantageously implemented by a fast and small area consuming hardware device for generating output bytes corresponding to respective input bytes according to a one-to-one binary function.

Independent Claim 17 is also directed to a method for generating output bytes, and is similar to independent Claim 12, but does not recite the 256-bit string.

Independent Claim 23 is directed to a device, and is similar to independent Claim 12.

Independent Claim 28 is directed to a cryptographic device, and is similar to independent Claim 12.

In re Patent Application of:

MACCHETTI ET AL.

Serial No. 10/816,791

Confirmation No. 9927

Filed: **APRIL 2, 2004**

II. The Claims Are Patentable

The Examiner rejected independent Claims 12, 17, 23 and 28 over the Coppersmith et al. patent. The Coppersmith et al. patent is directed to a symmetric key cipher for encryption and decryption, using a block cipher algorithm. The Examiner has taken the position that Coppersmith et al. discloses the claimed invention.

In terms of decoding an input byte and generating at least one bit string that contains only one active bit, the Examiner references the two s-boxes in FIG. 6. Each of the two s-boxes is a one-dimensional array of non-repeating values between 0 and 255. The s-boxes each have 256 entries, so that indexing can be performed with an 8-bit number. Reference is directed to column 8, line 62 through column 9, line 10 of Coppersmith et al., which provides:

"Each of the two s-boxes shown in FIG. 6 is a one-dimensional array of non-repeating values between 0 and 255, indexed from 0 to 255. (The s-boxes each have 256 entries, so that indexing can be performed with an 8-bit number, where 8 bits is the length of the value resulting from the two exclusive OR operations. Note that the values are shown in FIG. 6 using their decimal representation.) Referring again to the left-half mixing equation, it will be seen that when the byte counter i is an even number, s-box zero is used; when i is an odd number, s-box one is used. For example, when $i=2$, then $(i \bmod 2)=(2 \bmod 2)$, which evaluates to 0 and selects s-box zero; when $i=5$, then $(i \bmod$

In re Patent Application of:

MACCHETTI ET AL.

Serial No. 10/816,791

Confirmation No. 9927

Filed: **APRIL 2, 2004**

$2) = (5 \bmod 2)$, which evaluates to 1 and selects s-box one. The value retrieved from the s-box is substituted for the i th byte of original data from the current block, resulting in a mixed byte." (Emphasis added).

In terms of logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string, the Examiner references the equation in column 8, line 16, where C represents a block of data. In terms of encoding the 256-bit string for obtaining an output byte, the Examiner references column 9, line 22 which states that the functionality is provided by 2 boxes having 256 entries.

The Examiner further takes the position that access to the s-box array inherently expresses a 256-bit string whose active bit corresponds to an entry in the array. In terms of the encoding, the Examiner states that the 256-bit string is encoded to correspond to the actual substitution byte to be obtained.

The Applicants submit that the Examiner has mischaracterized the Coppersmith et al. patent. Coppersmith et al. discloses that the input byte (i.e., the "index") corresponds to a number from 0 to 255, and that this number corresponds to an output byte (i.e., a "mixed byte"). Coppersmith et al. does not disclose nor even suggest decoding the input byte into a 256 bit string that contains only one active bit.

Moreover, Coppersmith et al. fails to teach or suggest generating output bytes corresponding to respective input bytes according to a one-to-one binary function as in the claimed invention. Instead, Coppersmith et al. discloses that the value

In re Patent Application of:

MACCHETTI ET AL.

Serial No. 10/816,791

Confirmation No. 9927

Filed: **APRIL 2, 2004**

retrieved from the s-box is substituted for the ith byte of original data from the current block resulting in a mixed byte, as highlighted in the above quote from Coppersmith et al. When the byte counter i is an even number s-box zero is used, and when i is an odd number s-box one is used. The equation referenced by the Examiner in column 8, line 16, where C_i is defined, is thus used to generate a mixed byte that includes more than one active bit.

Accordingly, it is submitted that independent Claim 12 is patentable over the Coppersmith et al. patent. Independent Claims 17, 23 and 28 are similar to independent Claim 12. Therefore, it is submitted that these claims are also patentable over the Coppersmith et al. patent.

In view of the patentability of independent Claims 12, 17, 23 and 28, it is submitted that their dependent claims, which recite yet further distinguishing features of the invention, are also patentable. These dependent claims require no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

In re Patent Application of:


MACCHETTI ET AL.

Serial No. 10/816,791

Confirmation No. 9927

Filed: **APRIL 2, 2004**

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330